アプリケーション ユーザの設定

この章では、アプリケーション ユーザの情報を管理するための情報を提供します。

アプリケーション ユーザの設定の概要

Cisco Unified Communications Manager の管理ページで、[ユーザ管理(User Management)] > [アプリケーションユーザ(Application User)] メニュー パスを使用して、アプリケーション ポリシーを設定します。

Cisco Unified Communications Manager の管理ページの [アプリケーションユーザの設定(Application User Configuration)] ウィンドウを使用すると、管理者は Cisco Unified Communications Manager アプリケーション ユーザに関する情報を追加、検索、表示、および保持することができます。

アプリケーション ユーザの設定のヒント

[新規追加(Add New)] をクリックして新しいアプリケーション ユーザを設定します。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウのフィールドに入力して、アプリケーション ユーザの設定を行ってください。 詳細については、アプリケーション ユーザの設定値，（4 ページ）を参照してください。

（注） インストールの際に、Cisco Unified Communications Manager のデフォルトのアプリケーション ユーザ セットが提供されます。

（注） Cisco Unity または Cisco Unity Connection の管理者アカウントを追加する場合、Cisco Unity および Cisco Unity Connection Administration で定義したユーザ名とパスワードを使用する必要があります。ユーザ ID で、Cisco Unity または Cisco Unity Connection と Cisco Unified Communications Manager の管理との間の認証を行います。 Cisco Unity または Cisco Unity Connection 用の適切な『Cisco Unified Communications Manager Integration Guide』を参照してください。

[アプリケーションユーザの設定(Application User Configuration)] ウィンドウの [Cisco Unityアプリケーションユーザの作成(Create a Cisco Unity Application User)] オプションを使用して、Cisco Unified Communications Manager の管理アプリケーション ユーザを、Cisco Unity または Cisco Unity Connection のユーザとして設定できます。 その後で、Cisco Unity または Cisco Unity Connection の管理ページで追加の設定を行うことができます。

このアプリケーション ユーザのユーザ特権レポートを表示するには、[関連リンク(Related Links)] ドロップダウン リスト ボックスから [ユーザ特権レポート(User Privilege Report)] を選択し、[移動(Go)] をクリックします。

このアプリケーション ユーザの [ユーザ特権(User Privilege)] ウィンドウが表示されます。

このアプリケーションユーザのユーザ特権レポートを表示した後、このアプリケーションユーザの [アプリケーションユーザの設定(Application User Configuration)] ウィンドウに戻ることができます。 [ユーザ特権(User Privilege)] ウィンドウの [関連リンク(Related Links)] ドロップダウン リスト ボックスから [アプリケーションユーザに戻る(Back to Application User)] を選択し、[移動(Go)] をクリックします。

次の手順

デバイスをこのアプリケーションユーザに関連付ける、アプリケーションユーザのクレデンシャルを管理する、管理者ユーザを Cisco Unity または Cisco Unity Connection に追加する、といったことが可能です。

関連トピック

Cisco Unity または Cisco Unity Connection への管理者ユーザの追加 , （10 ページ）
アプリケーション ユーザのクレデンシャル情報の管理 , （12 ページ）
アプリケーション ユーザへのデバイスの関連付け , （15 ページ）
ユーザ権限、アクセス コントロール グループ、およびアクセス権の表示

アプリケーション ユーザの追加

アプリケーション ユーザを追加するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理ページで、[ユーザ管理(User Management)] > [アプリケーションユーザ(Application User)] を選択します。

ステップ 2 [新規追加(Add New)] をクリックします。

ステップ 3 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウのフィールドに入力し、[保存(Save)] をクリックします。 フィールドの説明については、アプリケーション ユーザの設定値，（4 ページ）を参照してください。

ステップ 4 [保存(Save)] をクリックします。

次の作業

デバイスをアプリケーションユーザに関連付けるには、アプリケーションユーザへのデバイスの関連付け，（15 ページ）を参照してください。

アプリケーション ユーザの削除

アプリケーションユーザを削除する前に、そのエンドユーザに関連付けられているデバイスまたはプロファイルを削除する必要があるかどうかを判断します。

アプリケーション ユーザに割り当てられているプロファイルおよび権限は、[アプリケーションユーザの設定(Application User Configuration)] ウィンドウの [CAPF情報(CAPF Information)] 領域および [権限情報(Permissions Information)] 領域から表示できます。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウで、[関連リンク(Related Links)] ドロップダウン リスト ボックスから [依存関係レコード(Dependency Records)] を選択することもできます。 依存関係レコードがシステムで使用できない場合は、[依存関係レコード要約(Dependency Records Summary)] ウィンドウにメッセージが表示されます。

次の手順

このユーザが Cisco Unity または Cisco Unity Connection で設定されている場合、Cisco Unified Communications Manager の管理ページでユーザを削除したときに、Cisco Unified Communications Manager に対するユーザの関連付けが破棄されます。 孤立したユーザは、Cisco Unity または Cisco Unity Connection の管理ページで削除できます。 詳細については、該当する『User Moves, Adds, and Changes Guide for Cisco Unity Connection』を参照してください。 Cisco Unity の詳細については、『System Administration Guide for Cisco Unity』を参照してください。

関連トピック

依存関係レコードへのアクセス

アプリケーション ユーザの設定値

以下の表では、アプリケーション ユーザの設定値について説明します。

表 *1*：アプリケーション ユーザの設定値

フィールド	説明
[アプリケーションユーザ情報(Application User Information)]	
[ユーザID(User ID)]	アプリケーション ユーザの固有の識別名を入力します。 Cisco Unified Communications Manager では、既存のユーザ ID を変更できます（LDAP サーバとの同期化を使用可能にしていない場合）。
[パスワード(Password)]	アプリケーション ユーザ パスワードとなる英数字または特殊文字を入力します。 割り当てられたクレデンシャル ポリシーで指定されている、最小文字数以上を入力する必要があります。 （注） アプリケーション ユーザの AXL パスワードを作成する時は、特殊文字を使用しないでください。
[パスワードの確認(Confirm Password、半角英数字のみ)]	ユーザ パスワードをもう一度入力します。
[ダイジェスト信用証明書(Digest Credentials)]	英数字文字列を入力します。 Cisco Unified Communications Manager は、ここで指定したダイジェスト信用証明書を使用して、SIP トランクの確認中に SIP ユーザ エージェントの応答を検証します。 ダイジェスト認証の詳細については『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。
[ダイジェスト信用証明書の確認(Confirm Digest Credentials)]	ダイジェスト信用証明書を正しく入力したことを確認するために、このフィールドにクレデンシャルを入力します。
[クレデンシャルの編集(Edit Credential)]	[クレデンシャルの編集(Edit Credential)] ボタンは、このユーザをデータベースに追加した後で表示されます。 このユーザのクレデンシャルを管理するには、このボタンをクリックします。

フィールド	説明
[プレゼンスグループ(Presence Group)]	このフィールドには、プレゼンス機能を設定します。 （注） このアプリケーション ユーザをプレゼンスで使用しない場合は、プレゼンス グループをデフォルト（[なし(None)]）設定のままにします。 ドロップダウン リスト ボックスから、アプリケーション ユーザ用のプレゼンス グループを選択します。 選択したグループによって、アプリケーション ユーザ（IPMASysUser など）がモニタできる対象が指定されます。 インストール時に、標準のプレゼンス グループが設定されます。 Cisco Unified Communications Manager の管理ページで設定されるプレゼンス グループも、ドロップダウン リスト ボックスに表示されます。 プレゼンス認証は、プレゼンス グループと連携して、グループ間のプレゼンス要求を許可またはブロックします。 グループ間の権限の設定の詳細については、『*Cisco Unified Communications Manager* 機能およびサービス ガイド』を参照してください。
[プレゼンスのSUBSCRIBEの許可(Accept Presence Subscription)]	このフィールドには、プレゼンス認証用のプレゼンス機能を設定します。 トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認証を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認証を行います。 Cisco Unified Communications Manager がこの SIP トランク アプリケーション ユーザからのプレゼンス要求を受け入れることができるようにするには、このチェックボックスをオンにします。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で[アプリケーションレベル認証を有効化(Enable Application Level Authorization)]チェックボックスをオンにしていない場合は、Cisco Unified Communications Manager によって、トランクに接続されている SIP ユーザ エージェントに 403 エラー メッセージが送信されます。 認証の詳細については『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。

フィールド	説明
[Out-of-Dialog REFERの許可(Accept Out-of-Dialog REFER)]	トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認証を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認証を行います。 Cisco Unified Communications Manager がこの SIP トランク アプリケーション ユーザからの Out-of-Dialog REFER 要求を受け入れることができるようにするには、このチェックボックスをオンにします。たとえば、SIP で開始される転送機能や他の高度な転送関連機能を使用するには、Cisco Unified Communications Manager がこのアプリケーション ユーザの着信 Out-of-Dialog REFER 要求を受け入れることができるようにする必要があります。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で[アプリケーションレベル認証を有効化(Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified Communications Manager によって、トランクに接続されている SIP ユーザ エージェントに 403 エラー メッセージが送信されます。 認証の詳細については『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。
[Unsolicited NOTIFYの許可(Accept Unsolicited Notification)]	トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認証を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認証を行います。 Cisco Unified Communications Manager がこの SIP トランク アプリケーション ユーザからの Unsolicited NOTIFY を受け入れることができるようにするには、このチェックボックスをオンにします。たとえば、メッセージ待機インディケータ（MWI）サポートを提供するには、Cisco Unified Communications Manager がこのアプリケーション ユーザの着信 Unsolicited NOTIFY を受け入れることができるようにする必要があります。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で[アプリケーションレベル認証を有効化(Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified Communications Manager によって、トランクに接続されている SIP ユーザ エージェントに 403 エラー メッセージが送信されます。 認証の詳細については『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。

フィールド	説明
[Replacesヘッダーの許可(Accept Replaces Header)]	トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で、アプリケーションレベルの認証を使用可能にした場合は、Cisco Unified Communications Manager がアプリケーションレベルの認証を行います。 Cisco Unified CM がこの SIP トランク アプリケーション ユーザからのメッセージのヘッダー置換を受け入れることができるようにするには、このチェックボックスをオンにします。たとえば、SIP トランク上の外部コールを、在席転送の場合と同様に、外部のデバイスまたは相手に転送するには、このアプリケーション ユーザの REFER および INVITE 内に Replaces ヘッダーを含む SIP 要求を Cisco Unified CM が受け入れることができるようにする必要があります。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウでこのチェックボックスをオンにしたが、トランクに適用される [SIPトランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] で [アプリケーションレベル認証を有効化(Enable Application Level Authorization)] チェックボックスをオンにしていない場合は、Cisco Unified CM によって、トランクに接続されている SIP ユーザ エージェントに 403 エラー メッセージが送信されます。 認証の詳細については『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。
[デバイス情報(Device Information)]	

フィールド	説明
[使用可能なデバイス(Available Devices)]	このリスト ボックスには、このアプリケーション ユーザとの関連付けに使用できるデバイスが表示されます。 デバイスをこのアプリケーション ユーザに関連付けるには、デバイスを選択し、このリスト ボックスの下にある下矢印をクリックします。 このアプリケーション ユーザに関連付けるデバイスがこのペインに表示されない場合は、次のボタンのいずれかをクリックして、他のデバイスを検索します。 • [別の電話を検索(Find more Phones)]：このアプリケーション ユーザに関連付ける他の電話機を検索する場合は、このボタンをクリックします。 電話機を検索するための [電話の検索/一覧表示(Find and List Phones)] ウィンドウが表示されます。 • [別のルートポイントを検索(Find more Route Points)]：このアプリケーション ユーザに関連付ける他のルート ポイントを検索する場合は、このボタンをクリックします。 コンピュータ/テレフォニー インテグレーション（CTI）ルート ポイントを検索するための [CTI ルートポイントの検索/一覧表示(Find and List CTI Route Points)] ウィンドウが表示されます。 • [別のパイロットポイントを検索(Find more Pilot Points)]：このアプリケーション ユーザに関連付ける他のパイロット ポイントを検索する場合は、このボタンをクリックします。 パイロット ポイントを検索するための [パイロットポイントの検索/一覧表示(Find and List Pilot Points)] ウィンドウが表示されます。
[制御するデバイス(Controlled Devices)]	このフィールドには、アプリケーション ユーザに関連付けられているデバイスのリストが表示されます。 デバイスを削除するには、デバイス名を選択し、このリスト ボックスの上にある上矢印をクリックします。 デバイスを追加するには、[使用可能なデバイス(Available Devices)] リスト ボックスでデバイスを選択し、下矢印をクリックします。
[CAPF情報(CAPF Information)]	

フィールド	説明
[割り当てられているCAPFプロファイル(Associated CAPF Profiles)]	このペインには、このユーザ用に設定したCAPFプロファイルのインスタンスIDが表示されます。 プロファイルを表示または更新するには、インスタンスIDをダブルクリックするか、インスタンスIDをクリックして選択してから [詳細の表示(View Details)] をクリックします。 [アプリケーションユーザCAPFプロファイルの設定(Application User CAPF Profile Configuration)] ウィンドウが表示され、現在の設定が表示されます。 アプリケーション ユーザ CAPF プロファイルの設定方法については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。
[権限情報(Permissions Information)]	
[グループ(Groups)]	このリスト ボックスは、アプリケーション ユーザ レコードが保存された後で表示されます。 このリスト ボックスには、アプリケーション ユーザが属するグループが表示されます。 ユーザを 1 つ以上のグループに追加するには、[アクセスコントロールグループに追加(Add to Access Control Group)] ボタンをクリックします。 [アクセスコントロールグループの検索/一覧表示(Find and List Access Control Groups)] ウィンドウが別ウィンドウで表示されます。 ユーザを追加するグループを見つけて、そのグループの横にあるチェックボックスをオンにします。次に、ウィンドウの下部にある [選択項目の追加(Add Selected)] をクリックします。 [アクセスコントロールグループの検索/一覧表示(Find and List Access Control Groups)] ウィンドウが閉じ、[アプリケーションユーザの設定(Application User Configuration)] ウィンドウが表示され、選択したグループが [グループ(Groups)] リスト ボックスに表示されます。 グループからユーザを削除するには、[グループ(Groups)] リスト ボックスでグループを選択し、[アクセスコントロールグループから削除(Remove from Access Control Group)] ボタンをクリックします。 グループを表示または更新するには、グループ名をダブルクリックするか、グループ名をクリックして選択してから [詳細の表示(View Details)] をクリックします。 [アクセスコントロールグループの設定(Access Control Group Configuration)] ウィンドウが表示され、現在の設定が表示されます。

フィールド	説明
[権限(Roles)]	このリスト ボックスは、アプリケーション ユーザが追加され、[グループ(Groups)] リスト ボックスにデータが入力され、ユーザ レコードが保存された後で表示されます。 このリストボックスには、アプリケーション ユーザに割り当てられている権限が表示されます。 権限を表示または更新するには、権限名をダブルクリックするか、権限名をクリックして選択してから [詳細の表示(View Details)] をクリックします。 [権限の設定(Role Configuration)] ウィンドウが表示され、現在の設定が表示されます。

関連トピック

アプリケーション ユーザの設定 , （1 ページ）
アプリケーション ユーザのクレデンシャル情報の管理 , （12 ページ）
権限の設定
アクセス コントロール グループの設定

Cisco Unity または Cisco Unity Connection への管理者ユーザの追加

[アプリケーションの設定(Application Configuration)] ウィンドウの [Cisco Unityアプリケーション ユーザの作成(Create Cisco Unity Application User)] リンクを使用すると、ユーザを管理者ユーザとして Cisco Unity または Cisco Unity Connection に追加することができます。 この方法を使用して、アプリケーション ユーザを Cisco Unified Communications Manager の管理ページで設定してから、そのユーザの追加設定を Cisco Unity または Cisco Unity Connection の管理ページで設定します。

Cisco Unified Communications Manager を Cisco Unity Connection 7.x に統合する場合は、この項で説明している手順を実行する代わりに、Cisco Unity Connection 7.x で使用可能なインポート機能を使用することができます。 インポート機能の使用方法の詳細については、『User Moves, Adds, and Changes Guide for Cisco Unity Connection 7.x』を参照してください。

[Cisco Unityユーザの作成(Create Cisco Unity User)] リンクが表示されるのは、該当する Cisco Unity または Cisco Unity Connection ソフトウェアのインストールと設定を行った場合だけです。 該当する『Cisco Unified Communications Manager Integration Guide for Cisco Unity』または該当する『Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection』を参照してください。

はじめる前に

Cisco Unity または Cisco Unity Connection にプッシュするユーザの適切なテンプレートを定義していることを確認します。 Cisco Unity Connection ユーザについては、該当する『User Moves, Adds,

and Changes Guide for Cisco Unity Connection』を参照してください。 Cisco Unity ユーザについては、『System Administration Guide for Cisco Unity』を参照してください。

手順

ステップ 1 アプリケーション ユーザを検索します。

ステップ 2 [関連リンク(Related Links)] ドロップダウン リスト ボックスから [Cisco Unityアプリケーションユーザの作成(Create Cisco Unity Application User)] リンクを選択し、[移動(Go)] をクリックします。 [Cisco Unityユーザの追加(Add Cisco Unity User)] ダイアログボックスが表示されます。

ステップ 3 [アプリケーションサーバ(Application Server)] ドロップダウン リスト ボックスから、Cisco Unity または Cisco Unity Connection ユーザを作成する Cisco Unity または Cisco Unity Connection サーバを選択し、[次へ(Next)] をクリックします。

ステップ 4 [アプリケーションユーザテンプレート(Application User Template)] ドロップダウン リスト ボックスから、使用するテンプレートを選択します。

ステップ 5 [保存(Save)] をクリックします。
Cisco Unity または Cisco Unity Connection に管理者のアカウントが作成されます。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウで、[関連リンク(Related Links)] 内のリンクが [Cisco Unityユーザの編集(Edit Cisco Unity User)] に変わります。 これで、Cisco Unity の管理ページまたは Cisco Unity Connection の管理ページに、作成したユーザが表示されるようになります。

（注） Cisco Unity ユーザまたは Cisco Unity Connection ユーザが Cisco Unified CM アプリケーション ユーザと統合された場合、[エイリアス(Alias)]（Cisco Unified Communications Manager の管理ページの [ユーザID(User ID)]）、[名(First Name)]、[姓(Last Name)]、[内線(Extension)]（Cisco Unified Communications Manager の管理ページの [プライマリ内線(Primary Extension)]）などのフィールドを、Cisco Unity の管理ページまたは Cisco Unity Connection の管理ページでは編集できません。 これらのフィールドは、Cisco Unified Communications Manager の管理ページでのみ更新できます。

（注） Cisco Unity および Cisco Unity Connection は、Cisco Unified Communications Manager からのデータの同期化をモニタします。 Cisco Unity の管理ページまたは Cisco Unity Connection の管理ページの [ツール] メニューで、同期時間を設定できます。 Cisco Unity Connection の詳細については、『User Moves, Adds, and Changes Guide for Cisco Unity Connection』を参照してください。 Cisco Unity については、『System Administration Guide for Cisco Unity』を参照してください。

関連トピック

アプリケーション ユーザの設定 , （1 ページ）

アプリケーション ユーザのパスワードの変更

アプリケーション ユーザのパスワードを変更する手順は、次のとおりです。

手順

ステップ 1 パスワードを変更するアプリケーション ユーザを見つけます。
[アプリケーションユーザの設定(Application User Configuration)] ウィンドウに、選択したアプリケーション ユーザの情報が表示されます。

ステップ 2 [パスワード(Password)] フィールドで、暗号化されている既存のパスワードをダブルクリックし、新しいパスワードを入力します。

ステップ 3 [パスワードの確認(Confirm Password、半角英数字のみ)] フィールドで、暗号化されている既存のパスワードをダブルクリックし、新しいパスワードをもう一度入力します。

ステップ 4 [保存(Save)] をクリックします。

関連トピック

アプリケーション ユーザの設定 , （1 ページ）

アプリケーション ユーザのクレデンシャル情報の管理

アプリケーション ユーザのクレデンシャル（関連付けられた認証ルール、関連付けられたクレデンシャル ポリシー、パスワードの最終変更時間など）を変更または表示する手順は、次のとおりです。 ユーザのクレデンシャルを編集できるのは、ユーザがデータベースに存在している場合だけです。

[クレデンシャル設定(Credential Configuration)] ウィンドウでは、割り当てられたクレデンシャル ポリシーと衝突する設定を保存することができません。 たとえば、ポリシーで [無期限(Never Expires)] チェックボックスがオンの場合、[クレデンシャル設定(Credential Configuration)] ウィンドウで [無期限にする(Does Not Expire)] チェックボックスをオフにして保存することはできません。ただし、[無期限(Never Expires)] ポリシー設定がオンでない場合、ユーザに別のクレデンシャル期限を設定することはできます（[無期限にする(Does Not Expire)] を含む）。この場合、ユーザ設定がポリシー設定よりも優先されます。

[クレデンシャル設定(Credential Configuration)] ウィンドウの他の設定と衝突する、[クレデンシャル設定(Credential Configuration)] ウィンドウの設定変更はできません。 たとえば、[ユーザは変更不可(User Cannot Change)] ボックスがオンの場合は、[ユーザは次回ログイン時に変更する必要あり(User Must Change at Next Login)] チェックボックスをオンにできません。

[クレデンシャル設定(Credential Configuration)] ウィンドウには、イベントのおよその回数が表示されます。このフォームは、次に認証クエリーまたはイベントが発生したときに更新されます。

はじめる前に

データベースにアプリケーション ユーザを作成します。

手順

ステップ 1 [アプリケーションユーザの検索/一覧表示(Find and List Application Users)] ウィンドウを使用して、アプリケーション ユーザの設定を検索します（[ユーザ管理(User Management)] > [アプリケーションユーザ(Application User)]）。
[アプリケーションユーザの設定(Application User Configuration)] ウィンドウに、設定情報が表示されます。

ステップ 2 パスワード情報を変更または表示するには、[パスワード(Password、半角英数字のみ)] フィールドの横にある [クレデンシャルの編集(Edit Credential)] ボタンをクリックします。 [クレデンシャル設定(Credential Configuration)] ウィンドウが表示されます。

ステップ 3 ユーザのクレデンシャルデータを表示するか、適切な設定値を入力します（表2：アプリケーションユーザおよびエンドユーザのクレデンシャルの設定値とフィールド，（13ページ） を参照）。

ステップ 4 設定値を変更した場合は、[保存(Save)] をクリックします。

クレデンシャルの設定値とフィールド

次の表では、エンドユーザおよびアプリケーションユーザのクレデンシャルの設定値について説明します。 これらの設定値は、アプリケーション ユーザまたはエンド ユーザのダイジェスト信用証明書には適用されません。

表 *2*：アプリケーション ユーザおよびエンド ユーザのクレデンシャルの設定値とフィールド

フィールド	説明
[管理者によるロック(Locked by Administrator)]	このアカウントをロックし、ユーザがアクセスできないようにするには、このチェックボックスをオンにします。 アカウントのロックを解除し、ユーザがアクセスできるようにするには、このチェックボックスをオフにします。 このチェックボックスは、クレデンシャル ポリシーでこのアカウント タイプに [管理者がロック解除を行う(Administrator Must Unlock)] が指定され、アカウントのロックアウトが発生した後で使用します。
[ユーザは変更不可(User Cannot Change)]	ユーザがこのクレデンシャルを変更できないようにするには、このチェックボックスをオンにします。 このオプションは、グループ アカウントに対して使用します。 [ユーザは次回ログイン時に変更する必要あり(User Must Change at Next Login)] チェックボックスがオンになっている場合は、このチェックボックスをオンにできません。

フィールド	説明
[ユーザは次回ログイン時に変更する必要あり(User Must Change at Next Login)]	次回のログイン時に、このクレデンシャルの変更をユーザに要求するには、このチェックボックスをオンにします。 このオプションは、一時的なクレデンシャルを割り当てた後で使用します。 [ユーザは変更不可(User Cannot Change)] チェックボックスがオンになっている場合は、このチェックボックスをオンにできません。
[無期限にする(Does Not Expire)]	このクレデンシャルの変更をユーザに要求しないようにするには、このチェックボックスをオンにします。 このオプションは、セキュリティの低いユーザまたはグループ アカウントに使用できます。 オンにしても、ユーザはいつでもこのクレデンシャルを変更できます。 このチェックボックスがオフの場合、関連付けられているクレデンシャル ポリシーの有効期限の設定が適用されます。 ポリシー設定で [無期限(Never Expires)] が指定されている場合は、このチェックボックスをオフにできません。
[ハック数のリセット(Reset Hack Count)]	このユーザのハック数をリセットして、[失敗したログイン試行によりロックされた時間(Time Locked Due to Failed Logon Attempts)] フィールドをクリアするには、このチェックボックスをオンにします。 ハック数は、クレデンシャルが不正なために認証に失敗すると増えます。 ポリシーで [ログイン失敗無制限(No Limit for Failed Logons)] が指定されている場合、ハック数は常に 0 になります。
[認証ルール(Authentication Rule)]	このユーザのクレデンシャルに適用するクレデンシャル ポリシーを選択します。
[最終変更時間(Time Last Changed)]	このフィールドには、このユーザのクレデンシャルが変更された最新の日時が表示されます。
[失敗したログイン試行(Failed Logon Attempts)]	このフィールドには、成功した最終ログイン、管理者によるこのユーザ クレデンシャルのハック数のリセット、または失敗したログイン試行回数のリセット期間経過の後、失敗したログイン試行回数が表示されます。
[失敗した最後のログイン試行時間(Time of Last Failed Logon Attempt)]	このフィールドには、このユーザのクレデンシャルでログイン試行が失敗した最新の日時が表示されます。
[管理者によりロックされた時間(Time Locked by Administrator)]	このフィールドには、管理者がこのユーザ アカウントをロックした日時が表示されます。 管理者がクレデンシャルのロックを解除すると、このフィールドはブランクになります。

フィールド	説明
[失敗したログイン試行によりロックされた時間(Time Locked Due to Failed Logon Attempts)]	このフィールドには、失敗したログイン試行によってユーザ アカウントがロックされた最新の日時が表示されます。 ハック ロックアウトの時間は、失敗したログイン試行回数が、適用されているクレデンシャルポリシーで設定されているしきい値を超えると設定されます。

アプリケーション ユーザへのデバイスの関連付け

はじめる前に

アプリケーション ユーザにデバイスを割り当てるには、そのユーザの [アプリケーションユーザの設定(Application User Configuration)] ウィンドウにアクセスする必要があります。 [アプリケーションユーザの検索/一覧表示(Find and List Application Users)] ウィンドウ（[ユーザ管理(User Management)] > [アプリケーションユーザ(Application User)]）を使用して、アプリケーション ユーザを検索します。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウが表示された後で、デバイスを割り当てる手順は、次のとおりです。

手順

ステップ 1 [使用可能なデバイス(Available Devices)] リスト ボックスで、アプリケーション ユーザに関連付けるデバイスを選択し、リスト ボックスの下にある下矢印をクリックします。 選択したデバイスは、[制御するデバイス(Controlled Devices)] リストボックスに移動します。

ステップ 2 使用可能なデバイスのリストを制限するには、[別の電話を検索(Find more Phones)] ボタン、[別のルートポイントを検索(Find more Route Points)] ボタン、または [別のパイロットポイントを検索(Find more Pilot Points)] ボタンをクリックします。

a) [別の電話を検索(Find more Phones)] ボタンをクリックすると、[電話の検索/一覧表示(Find and List Phones)] ウィンドウが表示されます。 検索を行って、このアプリケーション ユーザに関連付ける電話機を見つけます。

b) [別のルートポイントを検索(Find more Route Points)] ボタンをクリックすると、[CTIルートポイントの検索/一覧表示(Find and List CTI Route Points)] ウィンドウが表示されます。 検索を行って、このアプリケーション ユーザに関連付ける CTI ルート ポイントを見つけます。

c) [別のパイロットポイントを検索(Find more Pilot Points)] ボタンをクリックすると、[パイロットポイントの検索/一覧表示(Find and List Pilot Points)] ウィンドウが表示されます。 検索を行って、このアプリケーション ユーザに関連付けるパイロット ポイントを見つけます。

ステップ 3 アプリケーション ユーザに割り当てるデバイスごとに、前述のステップを繰り返します。

ステップ 4 割り当てを完了したら、[保存(Save)] をクリックして、アプリケーション ユーザにデバイスを割り当てます。

関連トピック

アプリケーション ユーザの設定 , （1 ページ）